From Theory to Practice: Autonomy, Privacy and the Ethical Assessment of ICT

William Bülow and Misse Wester

1. Introduction

The ethical issues in relation to new developments in information and communication technology (ICT) are often framed in terms of privacy (e.g. van den Hoven 2009; Rössler 2005; Nissenbaum 1998). Privacy is held to be an important value in western democracies, and it is argued that having a private sphere is a necessary condition for other democratic rights, such as liberty and integrity, and values such as autonomy (e.g. Rössler 2005). However due to developments in informational technology, large amounts of personal data are stored by different actors in society. While the phenomena of collecting personal data is not new, there are mainly two hings that have changed in the past decade or so: first, more information is being collected than ever before and secondly, information is not just stored but is subjected to some sort of analysis (Lyon, 2006). Information about individuals are collected as they act in the normal course of their public lives. Information is shared in transactions with retailers, using credit card, mail order companies etc. The use of RFID-tags and CCVV cameras in various context, including workplace and public sphers, as well as the widepread use of e-services and internet helps to increase the amount of information stored about individuals by various actors. Also, the means of collecting and storing data has other consequenses. While information is often collected by an individual, an agancy or organisation with which a person interacts, information about individual can be collected by secondary users who acquire information from either primary or secondary sources (Nissenbaum 1998).

As various forms of information technology are emerging and being used in various parts of our personal and public lives, it has become important to consider the ethical aspects and the assessment of the possible use of these technologies. To achieve this end, one must indentify how different sorts of information stored about individuals related to the issue of privacy. This paper highlights the complexity of informational privacy and its relation to autonomy and the ethical assessment various uses of information technology. It is argued that due to its connection to autonomy, together with the ambiguous nature of referential descriptions, the possible intrusions to privacy which a particular information technology may give raise to, are hard to assess. This implies that the use of ICT cannot be determined solely on the basis of what sort of information is collected. It must also consider whom the information is about, in what context it is given, for what purpose.

The paper proceeds as follows: In section 2 we will discuss the importance of privacy and its connection to autonomy. In section 3 we will discuss what sort of information should be protected. In section 4 we present four scenarios from a survey study conducted in Sweden 2010 and discuss how they relate to our overall argument. In the final section we sum up our conclusions.

2. The importance of privacy

Privacy is held to be important because of its connection to autonomy (e.g. Rössler 2005; Palm 2009). Protection of a person's privacy enables her to control the access to information,

how it is distributed and to whom, and is a precondition for leading an autonomous life. For instance, Rössler (2005) argues that "privacy protects autonomy in those respects in which the exercise of autonomy is dependent upon my control of the access of others to me, to my person, to my (reflections on) decisions and to information about me" (Rössler 2005: 73). Similarly, Palm (2009) suggests that a "failure to protect privacy is problematic for the reason that we thereby fail to secure the more fundamental value of autonomy" (Palm 2009: 240). On this view, if one desires to live one's life as an open book, one should be able to do so, and whether one want to restrict the access to different sorts of information, this should be respected. In either case, the protection of privacy entails that a person should be able to control information, as well as private areas (such as ones home) from the unwanted intrusion of others.

Seeing privacy as a precondition of autonomy, intrusions to a person's privacy is problematic because it limits or restricts that person's autonomy. The amount of information people have about a person often affects how that person will behave towards those people. People act upon certain expectations about the particular situation in which we act. Rössler (2005) uses the following example as an illustration: in the case of hidden video surveillance in public places persons have certain expectations concerning unfamiliar people whom they meet and have expectations on how they will behave. However, persons do not expect being recorded on film and thus being converted into something that can be used reproduced and shown in public irrespectively of time and place (Rössler 2005). If the person being recorded by hidden surveillance cameras knew of this, this person would possibly behave differently. On this view, the violation of the right to privacy is a violation to the person's autonomy. Also, characterizing violation of the right to privacy as a violation to the person's autonomy also shows how the case of hidden video surveillance would be a violation to autonomy even though the person is not aware of being filmed. For even though a person's behavior in public is self-determent, this behavior is only apparently so because it was made by the person under false assumptions (Rössler 2005).

Of course there are other reasons why a person might want to keep certain information privacy. Most straightforwardly, the protection of privacy helps to prevent various sorts of harm, including reputational harm and the risk of being victim for cybercrimes. As van den Hoven (2008) points out, certain harms cannot be inflicted (or at least not easily) without if certain information were not available, such as identity theft and stalking, and counts in favour of the protection of personal data. However, despite the fact that personal information is protected, the respect for personal autonomy implies that a certain form of surveillance can be problematic anyhow. Moreover, as large amounts of personal information are stored about various actors, individuals are continually giving up the control over their personal information. This may, as Rössler points out, come to limit their autonomy:

> If it can in principle no longer be taken for granted that one has control over one's informational self-determination or that one is not (constantly) being observed, and if, as a result, one must (constantly) present oneself as though one were being observed, the result is a loss of autonomy in terms of the authenticity of one's behaviour, which is turned into behaviour *as if*, that is alienated behaviour (Rössler 2005: 128-9).

Following the idea that the protection of privacy is a precondition of autonomy, we will now discuss some issues which may arise when assessing possible uses of ICT.

3. Which information should be protected?

In addition to its account of the value of privacy, a normative theory of privacy must be able to account for what sort of personal data should be worth protecting. In a series of papers philosopher Helen Nissenbaum has argued that information technologies raises new privacy issues which are seldom acknowledged by philosophical accounts of privacy. Information about individuals are collected as they act in the normal course of their public lifes. Information is shared in transactions with retailers when using credit card or when usingmail order companies. In addition, the new means of collecting and stroring data involves another layer of surveilience that builds upon them. While information is often collected by an individual, agancy or organisation which whom a person interacts, this new layer of surveilience involves a new category of users who acquire information from either primary or secondary sources (Nissenbaum 1998). While we do share this information freely it is possible to combine various sources based on personal data, consumer preferences, habits etc and it is possible to create a pretty good picture of an individual by combining various sources. This, Nissenbaum refers to as the problem of privacy in the public (e.g. 1998; 2004). While this is not conceived as classical instances of violation to privacy, Nissenbaum suggests that it is problematic because the aggregation of personal data can be harmful to personal integrity. Another issue is that even if individuals willingly share one set of information in one context, she might want to avoid access to it in another (Nissenbaum 1998).

Part of the problem which Nissenbaum aims to capture is that certain information, when shared in one context, may be unproblematic while being harmful when shared in another context of put together with other personal information. A similar point is illustrated when recognizing a basic ambiguity about descriptions. As, van den Hoven (2008) points out, it is possible to distinguish *attributory* and *referential* descriptions. "The young man who takes the metro every weekday 08 am" could have more than one individual satisfying the description and is an instance of attributory description. However, at the same time "The young man who takes the metro every weekday 08 am" can be used referentially, when we have a particular person in mind. It is important to note that both attributory and referential descriptions are figuring in epistemic and doxatic strategies to collect information on people, and are directly or indirectly related to expand our knowledge about them. In other words, they are both *identity-relevant information* (van den Hoven 2008). Moreover, a large amount of attributory descriptions may be referring.

As van den Hoven points out, the distinction between referential and attributory descriptions is important since much data that is collected through various ICT, such as RFID-technology and CCTV cameras do collect data which in itself is attributory. It is therefore troublesome that only referential information should be protected. Moor (2008) points out, that as technological revolution increase their social impacts, ethical problems will also increase. This, Moor argues, is not simply because more people are affected, but because inevitably, revolutionary technology will provide numerous opportunities for actions. Information technology is clearly such a technology, enabling individuals, organizations, governments and governmental agencies to gather and store large amounts of personal data. While the importance privacy issues have been discussed before the widespread use of information technology (e.g. Rachels 1975), the privacy issues in relation to ICT are different, mainly because the enable information to be collected in one context, stored and sooner reproduced in another and even combined.

Another problem with assessing which sort of information should be protected arises directly from the importance of privacy and its connection to autonomy. What is and what is not private information differ among individuals and different sorts of information may be

perceived as private by certain individuals while not to others. For instance, it is important to a Muslim woman not to show her hair and at time, hair is not a private matter to a Swedish woman. In similar vein, the protection of privacy as a precondition to autonomy implies that whatever information that relates, or can relate to an individuals' autonomy, that individual desire to the hold private, or as Rössler (2005) puts it:

> Not only should what a person divulges not find its way into the wrong context, but what she never wants to divulge in the first place should remain what it is – a private matter. The seclusion or secrecy into which she can withdraw represents a limit to any social relationship in which she finds herself, for in all such relationships she is entitled to informational privacy of this order, and this ultimate control over her self-presentation constitutes the condition for her autonomy. This is on the one hand because subjective chaos of thoughts, feelings, images, self-definitions and self-interpretations is constitutive in determining what discloses itself as essential to person's life and how it does so (Rössler 2005: 140).

While it may seem like an attractive conclusion, it is in fact dubious. Despite how much a person divulges certain information about oneself there may be other reasons, such as public safety, for which this information must be shared anyhow. However, as autonomy is the sacred value for which privacy must be protected, one must assume that almost any sort of information might be held to be private, not because it is of a certain class, but because it relates to a particular individuals self-determination.

Clearly, an ethical assessment of ICT must answer questions about what aspects of personal autonomy will be restricted and how likely would it be that personal autonomy is actually reduced (Rössler 2005). However, as this is mandatory, it ought to be clear that due to its connections to autonomy the possible risks to privacy poses by the use of ICT cannot be determined solely on the basis of what sort of information is collected. It must also consider whom the information is about, in what context it is given, for what purpose etc, i.e. an ethical assessment of ICT, such as surveillance cameras or the use of RFID-tags in passports, should be more context-sensitive. It remains, however, to be discussed how such a model for evaluation would look like.

As the ethical assessment of ICT should be context relative, we will now illustrate how acceptance of ICT is also dependent on various factors

4. Acceptance of various ICT solutions

In order to illustrate the perception and acceptance of ICT we present empirical data from a survey study distributed among a representative sample of the Swedish population from 2010. Here two technologies used for collecting personal data are selected, the use of positioning technologies in mobile phones and the use of RFID tags. These technologies each have two versions, and can be summarized in the following way:

RFID tags are used for two purposes, where the first is for public transportation where information about your travel routines are stored by your local transport provider. In the second scenario, RFID tags are used for tracking shipments with e.g., clothes. Once the clothes have reached the retailers, the RFID tag remains in the individual article of clothing where it can be scanned by other retailers and used for marketing purposes.

The second technology deals with global positioning systems (GPS) available in mobile phones. In this scenario two different versions were used to measure public acceptance, where

the fist was the possibility to use the GPS system to share your location over the Internet so that friends and family could track an individuals' movements and this information is shared on a voluntary basis by the person herself; in the second the police can under specific circumstances activate this function in order to track individuals without their consent. In these cases, the same technology is used and collects the same sort of information. What is different is who collects it and whether the individual do consent.

Overall, the results show these two technologies regardless of application are not widely desired by the public. However, as the sort of information is similar in all cases, there are differences in acceptance. The acceptance for the commercial use of RFID tags are seen as most privacy invasive and positioning by police authorities as least invasive. This implies that the purpose of gathering data matters to how technologies that are privacy invasive are perceived. The commercial use of RFID tags in clothes is seen as the most questionable and outrageous. However, most people would not do anything to avoid being subjected to these technologies – with the exception for RFID tags in clothes.

5. Conclusion

The protection of privacy is important because it is a precondition to personal autonomy and to control of information about ourselves is necessary in order to determine how we present ourselves in different contexts. However, as autonomy is a precondition for autonomy, it also gives rise to an epistemological problem when assessing the ethical acceptance of ICT. What is held to be private information to different individuals in different context. This, calls for more context sensitive evaluations of ICT when used in various parts of public life.

References

Etzioni, A. (1999). *The Limits of Privacy*, New York, Basic Books.

Lyon, D. (2006). *Surveillance, power and everyday life, Oxford Handbook of Information and Communication Technologies*, Oxford University Press.

Moor, J. (2008) "Why We Need Better Ethics for Emerging Technologies", in *Information Technology and Moral Philosophy*,(ed). van den Hoven, J and Weckert, J. Cambridge, Cambridge University Press

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public, *Law and Philosophy*, 17, 559-596

Nissenbaum, H. (2004). Privacy as Contextual Integrity, Washington Law Review, 79, 119-157.

Palm, E. (2009). "Securing privacy at work: the importance of contextualized consent", *Ethics and Information Technology 11:* 233-241

Rössler, B. (2005). *The Value of Privacy*, Cambridge, Polity Press.

van den Hoven, J. (2010). ”Information Technology, Privacy and the Protection of Personal Data”, in *Information Technology and Moral Philosophy*,(ed). van den Hoven, J and Weckert, J. Cambridge, Cambridge University Press